Curriculum

Deutsche Version 2.0

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

0. Einleitung

Dieses Curriculum soll Lehrenden als Leitfaden dienen, um einen Lehrgang zum Thema Informationssicherheitsmanagement (ISM) für Eigentümer bzw. Manager sowie Mitarbeiterinnen und Mitarbeitern von kleinen und mittleren Unternehmen (KMU) organisieren und durchführen zu können. Das Curriculum soll im Sinne eines guten Beispiels Anregung für die praktische Umsetzung geben. Jeder einzelne Kurs, der auf der Grundlage dieses Curriculums durchgeführt wird, erfordert jedoch Modifikationen und Anpassungen des Konzeptes hinsichtlich der Bedürfnisse und Erwartungen der jeweiligen Teilnehmer. Wenn Teilnehmer eine individuellere Betreuung benötigen oder wenn einige der aufgeführten Lerneinheiten von größerem Interesse für die Lernenden sind als andere, ist der Lehrende frei, Prioritäten entsprechend der Bedürfnisse der Gruppe zu setzten.

Das Curriculum besteht aus fünf Abschnitten:

1. die Kursbeschreibung (Kapitel 1) gibt einen Überblick über die zentralen Lernziele;
2. die Makroplanung des Kurses (Kapitel 2) enthält Angaben zu den 3 Qualifizierungsstufen, den Lernzielen jeder Stufe, sowie Vorschläge zur Gewichtung und Gestaltung von Online- und Präsenzeinheiten;
3. eine Beschreibung der Zielgruppe, der Voraussetzungen pro Qualifizierungsstufe sowie der allgemeinen Rahmenbedingungen (Kapitel 3);
4. eine Beschreibung geeigneter Methoden;
5. ein Vorschlag für die Organisation des Blended-Learning-Konzeptes (Kapitel 5).

1. Kursbeschreibung

Das Ziel dieses Kurses ist es, Eigentümer oder Geschäftsführer von kleinen und mittleren Unternehmen in der Planung und Umsetzung eines adäquaten Informationssicherheitskonzeptes (IS-Konzept) zu unterstützen. Im Laufe des Kurses soll diese Zielgruppe ein grundlegendes Verständnis von Informationssicherheit (IS) und relevantes Basiswissen erwerben sowie deren Anforderungen und rechtliche Rahmenbedingungen, strategische und organisatorische Ansätze und praktische Maßnahmen kennenlernen. Um unterschiedliche Voraussetzungen und Bedarfe gerecht werden zu können, ist die Qualifizierung in 3 Stufen gegliedert:
Stufe 1: Grundalgen
Stufe 2: Aufbau
Stufe 3: Fortgeschritten

Nach Abschluss der Stufe 1 haben Teilnehmer ein allgemeines Verständnis von Informationssicherheitsmanagement und wissen, warum es für Unternehmen wichtig ist.
Auf Stufe 2 erhalten die Teilnehmer einen Überblick über Maßnahmen die zur Sicherung von Informationen ergriffen werden können.
Teilnehmer, die Stufe 3 abgeschlossen haben, sind in der Lage, die Rolle des für die Informationssicherheit Verantwortlichen für ihr Unternehmen zu übernehmen.

Ein für die Informationssicherheit verantwortlicher Mitarbeiter sollte über die folgenden Fähigkeiten und Kompetenzen verfügen:

- Schadensfälle so gut wie möglich verhindern können
- Bestimmtheit und Effektivität bei der Entscheidungsfindung
- Zwei-Wege-Kommunikation (von oben nach unten und von unten nach oben)
- delegieren und Mitarbeiter einbeziehen können
- auch schwache Hinweise auf Schadenspotentiale wahrnehmen können
- ein Team bilden und führen können
- sich aktiv an betriebswirtschaftlichen Fragen beteiligen, in einer flexiblen und innovativen Rolle, die kontinuierlich besser integriert wird, um die Geschäftsprozesse zu unterstützen
- einnehmen einer vermittelnden Rolle und Position
- starke Aufmerksamkeit für Anomalien, die von anderen kommuniziert werden
- Strenge und Objektivität bei der Analyse von Messergebnissen
- Eine primäre Rolle in der Qualifizierung von Mitarbeiterinnen und Mitarbeitern sowie in der Kommunikation geeigneter Schutzmaßnahmen und Verhaltensweisen einnehmen können.

Der für die Informationssicherheit verantwortliche Mitarbeiter sollte in der Lage sein:

1. das grundlegende Konzept der Informationssicherheit und seine Bedeutung für KMU zu verstehen;
2. den Wert der Informationssicherheit für das Unternehmen zu kommunizieren, in dem das Verständnis und die Wahrnehmung von Sicherheit bei den Mitarbeiterinnen und Mitarbeitern durch geeignete Aktivitäten verbessert wird;
3. sicherzustellen, dass die Bedeutung des Faktors Mensch im Sicherheitsmanagement erkannt wird und strukturierte Trainingspläne für verschiedene Berufsgruppen entwickelt und umgesetzt werden;
4. die Ist-Situation der Geschäftsprozesse im Detail analysieren können, um den Überblick über die Organisationsstruktur und die technologische Architektur zu erhalten;
5. zu wissen, über welche IKT-Struktur das Unternehmen verfügt und durch welche potentiellen Gefährdungen diese bedroht sein kann;
6. potenzielle Risiken und die am besten geeigneten Gegenmaßnahmen zu kennen, um deren Auswirkungen mildern zu können, unter Berücksichtigung der Auflagen und Möglichkeiten des gesetzlichen Rahmens;
7. das Unternehmen angemessen auf Notfälle und mögliche, sich daraus ergebende Krisen, vorbereiten zu können;
8. einen Notfallplan zu verwalten, um die Geschäftsfähigkeit nach einem Sicherheitsvorfall schnell wieder herstellen zu können.

2. Makroplanung

Um den Lernprozess zu kontextualisieren ist die Qualifizierung in drei Handlungsfelder unterteilt: Planen, Durchführen, Managen. Die Handlungsfelder folgen in ihrer Gesamtstruktur dem pädagogische Konzept der sogenannten "vollständigen Handlung", die als Kreislauf bestehend aus den folgenden Schritten verstanden wird: Informieren, Planen, Entscheiden, Durchführen, Steuern und Auswerten.

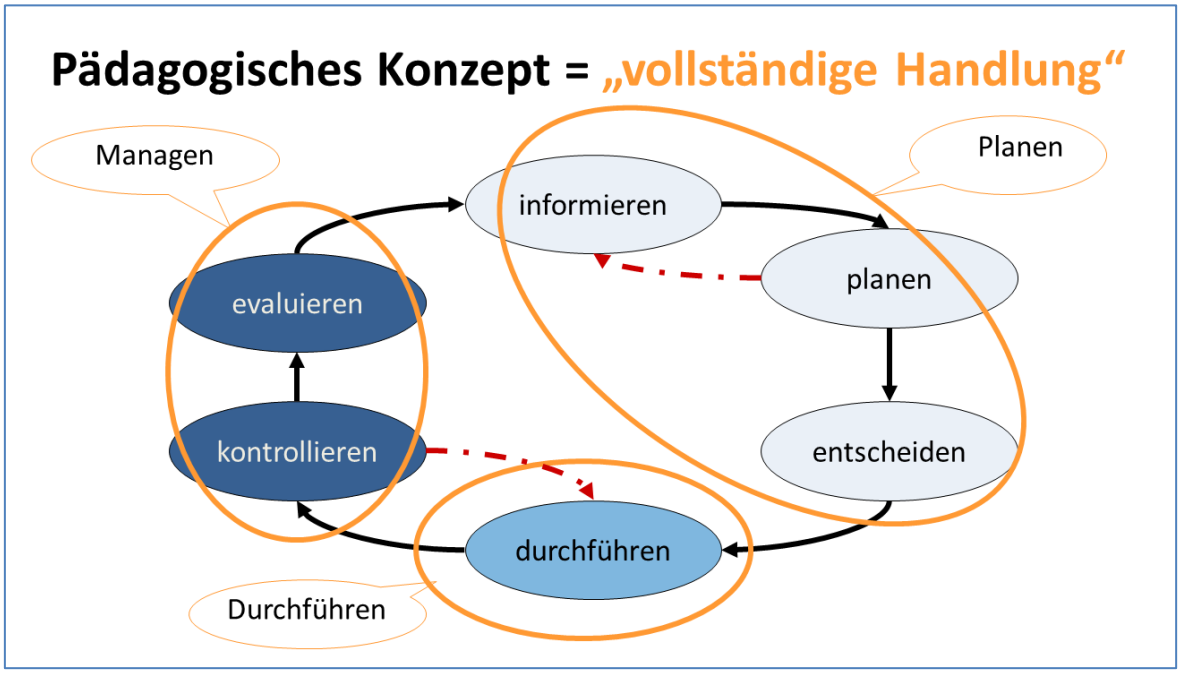

Abb. 1: Handlungsfelder und vollständige Handlung

2.1. Handlungsfelder

- Planen - Analyse der IST Situation und Entwicklung des IS-Konzepts
- Durchführen (operative Teilprozesse) – Bereitstellen, Beschaffen und Umsetzen bzw. Anwenden der erforderlichen Maßnahmen, Prozesse, Infrastruktur, Know-how
- Managen – Geschäftsprozesse optimieren, steuern und überwachen; Maßnahmen überprüfen, auswerten, anpassen und optimieren; Notfallpläne entwickeln

2.2. Qualifizierungsstufen

Der Workshop ist in 3 Qualifizierungsstufen unterteilt: Grundlagen, Aufbau und Fortgeschritten. Die hier benannten Lerneinheiten pro Stufe sowie deren Verteilung auf Online- und Präsenzeinheiten sind als Anregung zu verstehen und können, je nach Anforderung der konkreten Zielgruppe, variiert werden.

Stufe 1: Grundlagen
Zielgruppe: Inhaber bzw. leitende Angestellte und Mitarbeiter in KMU.

Lernziele / Kompetenzen: Das Hauptziel ist es, das Bewusstsein für Informationssicherheitsmanagement zu erhöhen und praktische Kenntnisse und Fähigkeiten aufzuzeigen, wie Informationssicherheit in den Unternehmensalltag integriert werden kann. Die Stufe 1 deckt Teile der Handlungsfelder Planung und Durchführung ab und besteht aus 15 Lerneinheiten.

Stufe 2: Aufbau
Zielgruppe: Inhaber bzw. leitende Angestellte von KMU, die verantwortlich für die Organisation der Informationssicherheit sind und Entscheidungsbefugnis haben.

Lernziele / Kompetenzen: Vorkenntnisse auf dem Gebiet der Informationssicherheit und IKT sind für Stufe 2 nicht erforderlich. Die Teilnehmer sollen in die Lage versetzt werden, Informationssicherheit für das eigene Unternehmen in enger Abstimmung mit einem externen Experten zu planen und zu organisieren. Entsprechend wird ein tiefergehendes Verständnis für die Planung und Implementierung von Informationssicherheit vermittelt. Stufe 2 besteht aus 15 Lerneinheiten.

Stufe 3: Fortgeschritten:
Zielgruppe: Inhaber bzw. leitende Angestellte von KMU, die einige IKT Vorkenntnisse haben sowie Vorkenntnisse in Sachen Informationssicherheit entsprechend der Stufen 1 und 2.

Lernziele / Kompetenzen: Ziel der Stufe 3 ist es, die Teilnehmer zu befähigen, Informationssicherheit im eigenen Unternehmen zu einem großen Teil selbstständig zu organisieren und geeignete Maßnahmen zu implementieren. Stufe 3 vermittelt zudem ein tieferes Verständnis für die strategischen Anforderungen und besteht aus 10 Lerneinheiten.

Die folgende Abbildung visualisiert die Struktur der Qualifizierungsstufen und stellt die Verteilung von Online- und Präsenzeinheiten dar.

Handlungs-felder	Stufe	Grundlagen		Aufbau		Fortgeschritten		
	Einheiten	online	Präsenz	online	Präsenz	online	Präsenz	
Planen		6	4	6	4			
Durchführen		3	2	3	2			
Managen						6	4	
Gesamt		9	6	9	6	6	4	
			15		**15**		**10**	**40**

Abb. 2: Struktur der Qualifizierungsstufen

2.3. Struktur der Handlungsfelder

Die Makroplanung wird in der unten stehenden Tabelle mit den folgenden Angaben beschrieben:

- Angabe der Qualifizierungsstufe
- Nennung des Handlungsfelds,
- Benennung der Lerneinheiten
- Anzahl der Lerneinheiten, wobei 1 Einheit 45 Minuten entspricht
- Kompetenzen, die in den gegebenen Lerneinheiten erreicht werden,
- Anregungen zu Lerninhalten, die geeignet sind, die genannten Kompetenzen zu fördern
- Vorschlag für die Aufteilung von Online- und Präsenzeinheiten

Stufe 1: Grundlagen

Planen (10 Einheiten)

Handlungsfeld **Lerneinheit** **Dauer**	**Kompetenzen**	**Präsenz-Inhalte**	**Online-Inhalte**
Informieren – Die Wichtigkeit von Informationssicherheit (IS) für das eigene Unternehmen verstehen 2 Einheiten	Die Teilnehmer verstehen die Wichtigkeit von Informationssicherheit für das eigene Unternehmen. Sie sind sich der möglichen Risiken bewusst, die entstehen, wenn die Informationssicherheit vernachlässigt wird. Die Teilnehmer kennen die rechtlichen Anforderungen und Vorschriften sowie die möglichen Sanktionen. Sie haben einen Überblick über relevante Gesetze und Vorschriften auf nationaler Ebene.	• Potentielle Risiken • Mögliche Folgen der Vernachlässigung der Informationssicherheit • Relevante nationale Gesetzte, Vorschriften und Normen sowie entsprechende Sanktionen • Techniken und Methoden, um auf dem neuesten Stand zu bleiben (z. B. Newsletter, RSS-Feeds)	CISO Modul 1 – Front Office
Informieren – Informationssicherheitsbedarf	Die Teilnehmer kennen relevante IKT-Schnittstellen zu Unternehmenswerten.	• Risikoanalyse • Identifizierung von EDV-	CISO Modul 2 – Back Office

des eigenen Unternehmens abschätzen und bewerten 1 Einheit		Schnittstellen zu relevanten Geschäftsprozessen	
Planen – Strategische Ziele der Informationssicherheit festlegen 1 Einheit	Die Teilnehmer sind in der Lage, strategische Ziele für die Umsetzung von Informationssicherheits-maßnahmen zu definieren. Die Teilnehmer sind in der Lage, Kriterien zur Bewertung der Maßnahmen zu definieren. Die Teilnehmer sind in der Lage, Ziele zu priorisieren.	Übungen zu SMARTen IS-Zielen: • Ziele SMART formulieren • ABC-Priorisierung von Zielen • Ziele unter Berücksichtigung der IS-Grundlagen formulieren	CISO Modul 3 – Back Office
Planen – IS Maßnahmenkatalog - auf Systemebene 2 Einheiten	Die Teilnehmer kennen arbeitsplatzbezogene IS-Maßnahmen und sind in der Lage, diese umzusetzen.	Praktische Übungen zu einzelnen Maßnahmen: • Wie erstelle ich ein sicheres Passwort • So konfigurieren Sie den Bildschirm sicherer	CISO Modul 1 – Front Office CISO Modul 4 – IT-Room
Planen – IS Maßnahmenkatalog - auf Netzwerkebene 2 Einheiten	Die Teilnehmer kennen wichtige IS-Maßnahmen auf Netzwerk- und Internet-Ebene.	• Sichere Nutzung von Web-Browsern • Sichere Internet-Nutzung • Sichere E-Mails	CISO Module 4 – IT-Room
Planen – IS Maßnahmenkatalog	Die Teilnehmer verstehen die Bedeutung des Faktors „Mensch“ im IS Kontext.	• Definition von Anforderungen z. B. bezüglich des	CISO Module 1 – Front Office CISO Module 2 – Back Office

- auf personeller Ebene 2 Einheiten		Arbeitsplatzes	
Ende des Moduls / Modulprüfung	Die Teilnehmer entwerfen einen IS-Maßnahmenkatalog einschließlich Umsetzungsplanung und Methoden. Sie begründen ihr Konzept mit Blick auf die Unternehmenswerte, die Anforderungen und das Kosten-Nutzen-Verhältnis, um die Aufrechterhaltung der Geschäftsfähigkeit gewährleisten zu können.		

Durchführen (5 Einheiten)

Handlungsfeld **Lerneinheit** **Dauer**	**Kompetenzen**	**Präsenz-Inhalte**	**Online-Inhalte**
Durchführen – Voraussetzungen für die Implementierung von IS klären 1 Einheit	Die Teilnehmer haben einen Überblick über aktuelle Sicherheitstechniken wie Authentifizierung und Kryptografie-Techniken.	• Aktuelle IS-Technologien und ihre Funktionalität	CISO Modul 1 – Front Office CISO Modul 4 – IT Room
Durchführen – Notfallmaßnahmen und Back-up-Konzept gestalten 1 Einheit	Die Teilnehmer kennen Maßnahmen, die im Fall eines Datenverlustes, Systemausfalls oder eines anderen Sicherheitsvorfalls zu ergreifen sind, um die Geschäftsfähigkeit in möglichst kurzer Zeit wieder herzustellen.	• Begründung und Zielsetzung des Notfallplans • Anforderungen an Notfall-maßnahmen • Anforderungen an die Datensicherung	CISO Module 3 – IS Office CISO Module 4 – IT Room
Durchführen – Support und Wartung 1 Einheit	Die Teilnehmer kennen die Anforderungen an die Wartung und den Support von Back-up-Lösungen.	• Supportintervalle • Up-dates	CISO Modul 4 – IT Room
Durchführen – Kontrollmechanismen implementieren	Die Teilnehmer haben einen allgemeinen Überblick über Kontrollmechanismen. Sie sind in der Lage, zwischen diesen Maßnahmen zu unterscheiden.	• Auswahl von Maßnahmen und Bewertung von deren Vor-und Nachteilen	CISO Modul 3 – IS Office

1 Einheit			
Durchführen – Tests durchführen 1 Einheit	Die Teilnehmer kennen Tests, die geeignet sind, um die Wirksamkeit der IS-Maßnahmen zu überprüfen.	• Wie kann man auf sich verändernde Sicherheitsanforderungen reagieren?	
Ende des Moduls / Modulprüfung	Die Teilnehmer erstellen einen Kriterienkatalog zur Implementierung von IS im eigenen Betrieb. Sie identifizieren und beschreiben besonders sensible Vermögenswerte.		

Stufe 2: Aufbau

Planen (10 Einheiten)

Handlungsfeld **Lerneinheit** **Dauer**	**Kompetenzen**	**Präsenz-Inhalte**	**Online-Inhalte**
Informieren – Die Wichtigkeit von Informationssicherheit verstehen 1 Einheit	Die Teilnehmer haben einen Überblick über relevante Gesetzte und Vorschriften auf europäischer Ebene.	• Relevante Europäische Gesetze und Normen	CISO Modul 1 – Front Office CISO Modul 3 – IS Office
Informieren – Den konkreten Informationssicherheitsbedarf des eigenen Unternehmens ermitteln Risikoanalyse 2 Einheiten	Die Teilnehmer sind in der Lage, Informationen als Vermögenswerte des Unternehmens und zentrale Geschäftsprozesse zu identifizieren und diese im Hinblick auf ihre Bedeutung für die Aufrechterhaltung der Geschäftsfähigkeit und Wettbewerbsfähigkeit zu bewerten. Die Teilnehmer sind in der Lage das Ausmaß eines möglichen Verlust oder einer Beschädigung von Daten zu	Risikoanalyse • ABC-Priorisierung von Geschäftsprozessen und Unternehmenswerten (Informationen) • Ermittlung der Zeitspanne, innerhalb der nach einem IKT Ausfall oder Datenverlust gehandelt werden muss • Benennen und Schätzen des potenziellen Verlusts	CISO Modul 2 – Back Office

	beziffern.		
Planen – IS-Maßnahmenkatalog - auf Systemebene 2 Einheiten	Die Teilnehmer kennen Sicherheitsmaßnahmen auf Systemebene und sind in der Lage diese bei Bedarf anzupassen und zu konfigurieren. Die Teilnehmer haben einen Überblick über geeignete IKT-Lösungen, um System basierte Sicherheitsmaßnahmen zu ergänzen. Die Teilnehmer verstehen das Prinzip der Benutzerrollen.	Praktische Übungen zu folgenden Themen: • Betriebssystem konfigurieren • Erkennung von Malware • Benutzerrollen und deren Rechte und Pflichten • IKT-Lösungen für IS	CISO Modul 4 – IT Room
Planen – IS-Maßnahmenkatalog - auf Netzwerkebene 2 Einheiten	Die Teilnehmer verstehen die Prinzipien der Netzwerksicherheit.	• Firewall	CISO Modul 4 – IT Room
Planen – IS-Maßnahmenkatalog - auf personeller Ebene 1 Unit	Die Teilnehmer kennen geeignete Maßnahmen, um Mitarbeiter aktiv in IS-Maßnahmen einzubeziehen, wie z. B. interne Kommunikation, gute Beispiele, Bonussysteme.	• Definition und Kommunikation von Regeln und Vorschriften sowie Sanktionen • Maßnahmen zur Sensibilisierung der Mitarbeiter für IS • Schulungsbedarf von Mitarbeitern erkennen.	CISO Modul 2 – Back Office

Entscheiden – Kosten-Nutzen-Analyse von IS-Maßnahmen 2 Einheiten	Die Teilnehmer sind in der Lage, das Kosten-Nutzen-Verhältnis der einzelnen IS Maßnahmen zu ermitteln und auf dieser Grundlage über die Umsetzung einzelner Maßnahmen zu entscheiden.	• Berechnung der Kosten einzelner IS Maßnahmen • Abschätzung des Nutzens einzelner IS Maßnahmen • Abschätzung des potenziellen finanziellen Risikos durch Beschädigungen oder Verlust von Informationen und Vergleich mit den Kosten einzelner IS Maßnahmen	CISO Modul 2 – Back Office
Ende des Moduls / Modulprüfung	Die Teilnehmer entwerfen einen IS Maßnahmenkatalog einschließlich Umsetzungsplanung und Methoden und begründen ihre Entscheidung mit Blick auf die Vermögenswerte (Informationen) des eigenen Unternehmens sowie der Anforderungen zur Aufrechterhaltung der Geschäftsfähigkeit und der Kosten-Nutzen-Analyse.		

Durchführen (5 Einheiten)

Handlungsfeld **Lerneinheit** **Dauer**	**Kompetenzen**	**Präsenz-Inhalte**	**Online-Inhalte**
Durchführen – Voraussetzungen für die Umsetzung von IS-Maßnahmen klären 1 Einheit	Die Teilnehmer sind in der Lage, verschiedene Reporting-Systeme zu aktivieren.	• Arbeitsprinzipien und Funktion von Betriebssystemen.	CISO Modul 4 – IT Room
Durchführen – Notfallmaßnahmen und Back-up-Konzepte definieren 1 Einheiten	Die Teilnehmer sind in der Lage, über geeignete Notfall- und Back-up-Maßnahmen für ihr Unternehmen zu entscheiden.	• Notfallplan	CISO Modul 3 – IS Office
Durchführen – Support und Administration 1 Einheit	Die Teilnehmer verstehen die Anforderungen an eine effektive und effiziente Wartung von IS-Maßnahmen. Die Teilnehmer sind in der Lage, ein geeignetes Management-Konzept zu entwickeln und umzusetzen.	• Supportintervalle • Up-dates	CISO Modul 3 – IS Room CISO Modul 4 – IT Room
Durchführen – Kontrollmechanismen	Die Teilnehmer sind in der Lage, Kriterien zu definieren, um die Umsetzung von IS	• Kontrollintervalle definieren • Kontrollkriterien festlegen	CISO Modul 3 – IS Office

umsetzen 1 Einheit	Maßnahmen zu steuern.		
Durchführen – Kooperation mit Experten 1 Einheit	Die Teilnehmer sind in der Lage zu definieren, bis zu welchem Grad und für welche Aufgabe die Zusammenarbeit mit externen Experten notwendig ist. Die Teilnehmer sind in der Lage eine Anfrage an externe IS-Experten zu formulieren und verschiedene Angebote zu vergleichen.		
Ende des Moduls / Modulprüfung	Die Teilnehmer erstellen einen Kriterienkatalog zur Umsetzung von IS im eigenen Betrieb. Sie identifizieren und beschreiben besonders sensible Vermögenswerte.		

Stufe 3: Fortgeschritten

Managen (10 Einheiten)

Handlungsfeld **Lerneinheit** **Dauer**	**Kompetenzen**	**Präsenz-Inhalte**	**Online-Inhalte**
Kontrollieren – Dokumentation von IS Maßnahmen 1 Einheit	Die Teilnehmer verstehen die Notwendigkeit der Dokumentationen von IS Maßnahmen. Die Teilnehmer kennen und verstehen konkrete Anforderungen an diese Dokumentation.	• Nutzen und Zweck der Dokumentation • Anforderungen an die Dokumentation • Aktualisierungsintervalle	CISO Modul 3 – IS Office
Kontrollieren – Schulungsbedarfe ermitteln 2 Einheiten	Die Teilnehmer verstehen und wissen, warum und wann Schulungsbedarfe entstehen. Sie sind in der Lage, Anforderungen an eine geeignete Qualifizierung zusammen mit ihren Mitarbeitern zu definieren. Die Teilnehmer wissen, wo Sie Informationen und Beratung zu Qualifizierungsangeboten finden können.	• Methoden zur Beurteilung des Schulungsbedarfs • Informationsquellen und Beratungsangebote zu ISM-Qualifikation	CISO Modul 2 – Back Office CISO Modul 3 – IS Office
Kontrollieren –	Die Teilnehmer kennen	Informationsquellen und	

Anpassung an gesetzliche Veränderungen 1 Einheit	Quellen, um sich über die Aktualisierung relevanter Gesetze auf dem Laufenden zu halten. Die Teilnehmer sind in der Lage, bereits umgesetzte Maßnahmen hinsichtlich der juristischen Veränderungen zu bewerten und sie entsprechend anzupassen.	rechtlichen Grundlagen zum Thema ISM	
Evaluieren – Das strategische ISM-Konzept evaluieren und anpassen 2 Einheiten	Die Teilnehmer sind in der Lage, das strategische ISM Konzept hinsichtlich der Veränderung von Geschäftsprozessen, technologischer Rahmenbedingungen oder juristischer Anforderungen anzupassen.	• Grundlagen des strategischen ISM • Intervalle für die Bewertung und Anpassung der IS Strategie • PDCA-Methode	CISO Modul 3 – IS Office
Evaluieren – Zukunftsorientierung 2 Einheiten	Die Teilnehmer sind in der Lage die potenziellen Auswirkungen technologischer Entwicklungen und weiterer Innovationen auf die Geschäftsprozesse und die Organisation zu beurteilen zu und bewerten. Die Teilnehmer sind in der Lage mittelfristige Change	• Aktuelle Trends, z. B. mobiles Arbeiten, Cloud Computing • Probleme, die während der Umsetzung von Trends auftreten könnten • entscheiden, welchen Trends gefolgt wird	

	Management Prozesse zu entwerfen.		
Evaluieren – Audits / Qualitätsmanagement 2 Einheiten	Die Teilnehmer sind in der Lage, die Wirksamkeit von IS Steuerungsinstrumenten zu beurteilen. Die Teilnehmer verstehen Nutzen und Zweck von Audits und sind in der Lage, den informativen Wert eines Zertifikats abzuschätzen. Die Teilnehmer kennen wichtige Kriterien für die Beauftragung eines Audits.	• Nutzen und Zweck von Audits • Informativer Wert der Zertifikate • Anforderungen an Audits • Juristische Grundlagen	
Ende des Moduls / Modulprüfung	Die Teilnehmer reflektieren das ISMS und den Notfallplan um die Strategie und Umsetzung des IMS zu aktualisieren / optimieren.		

3. Voraussetzungen und Rahmenbedingungen

3.1. Voraussetzungen der Zielgruppe

Die Beschreibung der angenommenen Voraussetzungen der Teilnehmer erfolgt unter Berücksichtigung aller Merkmale der Zielgruppe, die den Lernprozess entweder positiv oder negativ beeinflussen können. Im Einzelfall ist die Zielgruppenbeschreibung entsprechend der tatsächlichen Voraussetzungen der Lernenden anzupassen.

Stufe 1 – Grundlagen:

- Inhaber / Führungskräfte / mitarbeitende Partner
- Mitarbeiter
- keine IS Vorkenntnisse
- IKT- Grundkenntnisse, Anwenderwissen
- Männer und Frauen
- heterogene Altersstruktur – bei jüngeren Teilnehmern kann eine eher fortgeschrittene IKT-Kompetenz angenommen werden
- verschiedene Bildungsniveaus / Lehrlingsausbildung / Fachkräfte / akademischer Grad / Meister usw.
- Teilnehmer sind in der Regel in Vollzeit berufstätig

Stufe 2 – Aufbau:

- Inhaber / Führungskräfte / mitarbeitende Partner
- IKT-Grundkenntnisse, Anwenderwissen
- Männer und Frauen
- heterogene Altersstruktur – bei jüngeren Teilnehmern kann eine eher fortgeschrittene IKT-Kompetenz angenommen werden
- verschiedene Bildungsniveaus / Lehrlingsausbildung / Fachkräfte / akademischer Grad / Meister usw.
- Teilnehmer sind in der Regel Vollzeit berufstätig
- Vorkenntnisse entsprechend der Inhalte der Grundlagenstufe

Stufe 3 – Fortgeschritten:

- Inhaber / Führungskräfte / mitarbeitende Partner
- Vorkenntnisse entsprechend der Inhalte des Grundlagen- und Aufbaumoduls
- mittlere bis fortgeschrittene IKT-Kenntnisse / mittlere bis fortgeschrittene Kenntnisse über IKT-Support, Netzwerk-Management usw.
- Männer und Frauen
- heterogene Altersstruktur – bei jüngeren Teilnehmern kann eine eher fortgeschrittene IKT-Kompetenz angenommen werden
- verschiedene Bildungsniveaus / Lehrlingsausbildung / Fachkräfte / akademischer Grad / Meister usw.

Rahmenbedingungen

Die Beschreibung der Lernumgebung erfolgt unter Berücksichtigung aller Rahmenbedingungen, die den Lernprozess im Präsenzunterricht wie auch in der Online-Phase entweder positiv oder negativ beeinflussen können. Folgende Aspekte sind als Beispiele gedacht. Eine Anpassung dieser Beschreibung an die tatsächlichen Bedingungen ist im Einzelfall erforderlich.

- Mindestteilnehmerzahl: 7-10
- Anforderungen an die Ausstattung des Seminarraums:
  - Reguläre Seminarausstattung (z. B. Beamer, Laptop, Internetanschluss, Flipchart, Metaplan Material);
  - Raum für Gruppenarbeit
- Anforderungen an die Online-Lern-Phase (Teilnehmer):
  - PC oder Laptop mit Flatrate Internet-Anschluss
- aktuellen Browser,
- Anforderungen an die Online-Lehr-Phase (Lehrer):
  - Tutor
  - Helpdesk
- heterogene IKT-Strukturen in den Unternehmen = erfordert individuelle IS-Konzepte

4. Ausgewählte Methoden

Die Methoden, die im Unterricht eingesetzt werden, sollen die Lernenden dabei unterstützen, die folgenden Grundfertigkeiten zu erwerben:

- die Ist-Situation des Unternehmens analysieren können
- Bedürfnisse und Möglichkeiten zur Optimierung erkennen können
- Schulungs- und Beratungsbedürfnisse der Mitarbeiter identifizieren können
- Anforderungen an die Informationssicherheit definieren können
- implementierte Lösungen und Prozesse steuern und überwachen können sowie Handlungsbedarf erkennen können
- Prozesse dokumentieren können

Die folgenden Methoden sind geeignet, um im Unterricht die benötigten methodischen Fähigkeiten zu vermitteln sowie die beschriebenen Lernziele zu realisieren:

- Meta-Plan
- Mind Mapping
- Ursache-Wirkungs-Diagramm (auch Ishikawa-Diagramm)
- 4-Felder-Methode
- PDCA Verfahren nach ISO
- Rollenspiele
- Fallbeispiel „Unternehmen mit Mängeln im IS-Management“
- usw.

4.1. Vorbereitung auf das selbstständige Lernen

Da nicht jeder Lerner mit Internet-basierten Lernformen bzw. selbstständigem Lernen vertraut ist, kann es notwendig sein, die Lernenden diesbezüglich zu unterstützen. Folgende Maßnahmen und Methoden sind dazu geeignet:

- Organisation des Unterrichts entlang der Phasen einer „vollständigen Handlung“ (informieren, planen, entscheiden, ausführen, überwachen, auswerten)
- thematische Prioritäten in Absprache mit den Lernenden setzen
- Lernstrategien vermitteln, um die Lernenden bei der Reflexion und Analyse des bisherigen Lernverhaltens zu unterstützten
- Methoden anbieten, mit denen Lernbedarfe (eigene und von anderen, z. B. Mitarbeiter) erkannt werden können
- Ausreichend Zeit für die Behandlung der einzelnen Themen einplanen
- Vielfalt der Methoden und Formen der sozialen Interaktion je nach Bedarf der Lerngruppe ausschöpfen (z. B. individuelles Lernen, Teamarbeit, Kreativitätstechniken, strukturellen und organisatorischen Methoden, analytische Methoden und Entscheidungsfindung Tools)

4.2. Orientierung der Lernenden

Da der Kurs für eine Zielgruppe konzipiert ist, die über berufliche Erfahrung verfügt, ist es wichtig, diese Erfahrungen in den Unterricht zu integrieren. Dies kann durch die folgenden Methoden erreicht werden:

- bewusstes aufgreifen der Voraussetzungen und Vorkenntnisse und aktive Beteiligung der Teilnehmer am Unterricht
- Berücksichtigung individueller betrieblicher Prozesse und Strukturen der verschiedenen Unternehmen
- geeignete Beispiele und Analogien

4.3. Lernzielvereinbarung mit den Lernenden

Außerdem ist die Vereinbarung von Lernzielen zu Beginn des Kurses eine nützliche Methode Erfahrungen und Kompetenzen der Lernenden in den Unterricht zu integrieren:

- Abfrage der Bedürfnisse und Erwartungen der Lernenden an den Unterricht
- schriftlich vereinbaren, welche Themen abgedeckt werden sollen
- vereinbaren, welcher Beitrag von den Lernenden zum Gelingen des Unterrichts erwartet wird
- klären, welchen Unterstützungsbedarf die Lernenden sehen
- gemeinsame Regeln für die Zusammenarbeit vereinbaren und festlegen.

4.4. Verteilung der Aktivitäten

Da die Lernenden aktiviert und unterstützt werden sollen, selbstständig zu lernen, ist die folgende Verteilung der Aktivitäten zwischen Lehrendem und Lernenden hilfreich:

- der Lehrende plant und bereitet den Unterricht vor, wählt Methoden, Materialien und Medien aus und entwickelt Aufgaben
- der Lehrende sollten nicht als Dozent agieren; grundlegende theoretische Informationen sollten in erster Linie über das Internet vermittelt werden, zusammen mit Selbsttests und kurzen Übungen, um den Lernfortschritte zu sichern; die Präsenzlehre sollte in erster Linie für praktische Übungen und die Anwendung der erlernten Grundlagen verwendet werden; komplexe Übungen sichern die Fähigkeit, das neu erworbene Wissen auf neue Situationen anzuwenden
- der Lehrende moderiert den Lernprozess, d. h. er / sie beobachtet und bietet Beratung und Unterstützung je nach Bedarf an
- die Lernenden sind aktiv in den Lernprozess eingebunden; sie verwenden die bereitgestellten Medien und Materialien und erarbeiten Lösungen für die gestellten Lernaufgaben

4.5. Zu erwartende Lernschwierigkeiten

Aufgrund der zu erwartenden heterogenen Lerngruppen und den unterschiedlichen Voraussetzungen der einzelnen Teilnehmer, ist das Auftreten von Lernschwierigkeiten sehr wahrscheinlich. Ausgehend von dem Thema des Kurses sind Schwierigkeiten u. a. in den folgenden Bereichen zu erwarten:

- IKT-Kompetenz
- Rechtliche Fragen
- Heterogene Voraussetzungen der Teilnehmer
- Die Teilnehmer werden wahrscheinlich nicht bereit sein, offen über Informationssicherheit im eigenen Unternehmen zu sprechen

4.6. Lernerfolgssicherung und erwachsenengerechtes Prüfen

Da es das Ziel dieses Curriclums ist, eine kontextualisierte und praxisorientierte Qualifizierung zu gewährleisten, sollten Tests zur Lernerfolgssicherung und Abschlusstests diesem Anspruch ebenfalls gerecht werden.

- Verständnisfragen zur Sicherung des neu gewonnenen Wissen, z. B. Multiple-Choice
- Transfer von Wissen / Anwendung von Wissen in veränderten Kontexten (z. B. im Rahmen des Unterrichts)
- Anwendung von Wissen in komplexen Projekten, wie zum Beispiel die Erstellung eines Sicherheitskonzepts für das eigene Unternehmen
- Präsentation und Diskussion der Ergebnisse vor den Lehrenden und / oder der Lerngruppe

5. Blended-Learning-Konzept

Der Kurs ist als so genanntes Blended-Learning-Konzept geplant, was bedeutet, dass einige Einheiten im Präsenzunterricht und einige online vermittelt werden. Das vorliegende Curriculum wurde so geplant, dass etwa 1/3 der Ausbildung (16 Einheiten) in Präsenz und 2/3 (24 Einheiten) online geschult werden. Das folgende Bild stellt einen Vorschlag dar, wie der Unterricht entsprechend dieser Einteilung organisiert werden kann. Die Struktur ist nicht obligatorisch, sondern soll als Beispiel und Anregung dienen.

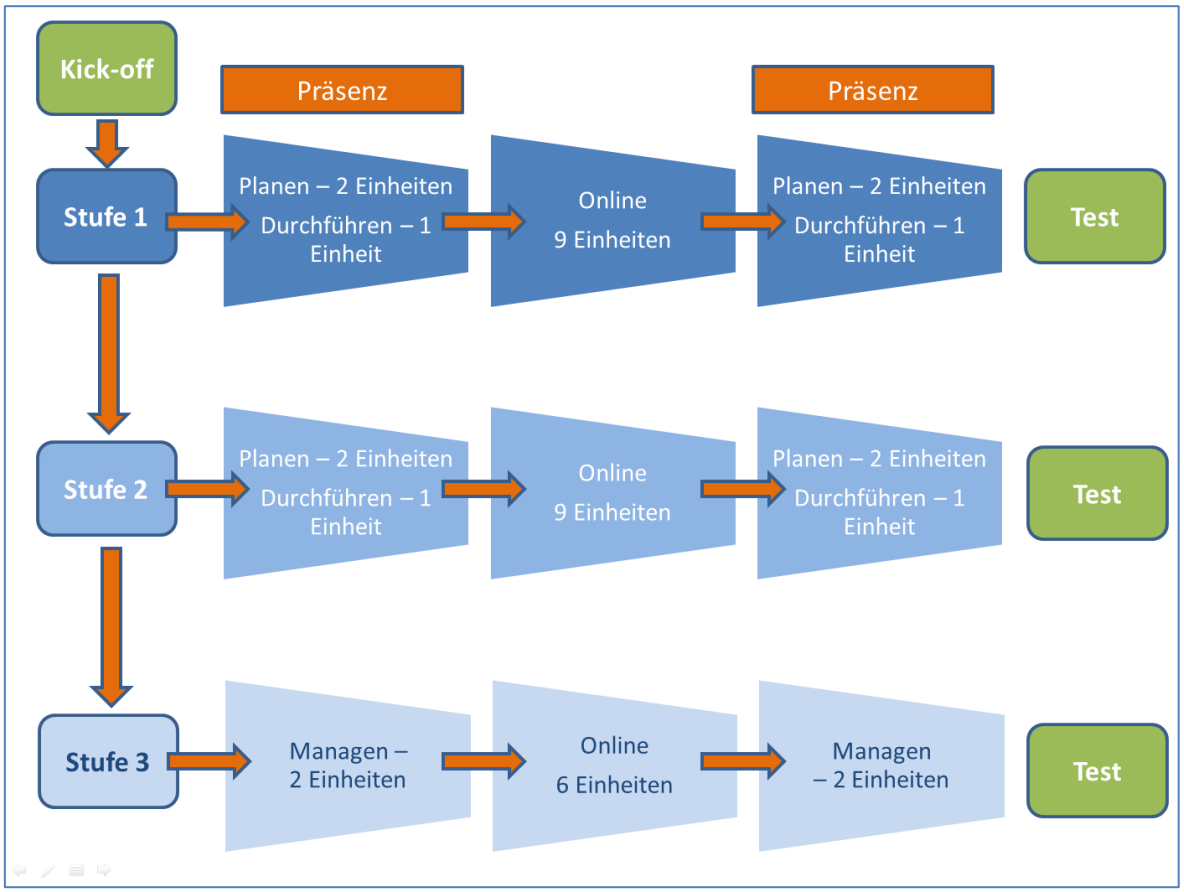

Abb. 3: Blended-Learning-Konzept

Hinsichtlich der unterschiedlichen Bedürfnisse und Erwartungen der Zielgruppe ist eine andere Verteilung von Online- und Präsenzeinheiten grundsätzlich möglich.

Da nicht zu erwarten ist, dass alle Teilnehmer mit Blended-Learning-Konzepten im Allgemeinen oder der eingesetzten Lernumgebung im Besonderen vertraut sind, wird eine Kick-off-Veranstaltung empfohlen, in der beides erklärt und eingeführt wird. Die Kick-off-Veranstaltung ist zudem für die Teilnehmer und Trainer eine Gelegenheit sich kennen zu lernen. Die für das Kick-off benötigte Zeit ist nicht in den geplanten 40 Trainingseinheiten enthalten.

Am Ende eines jeden Moduls wird ein Test bzw. eine Prüfung empfohlen, um sicherzustellen, dass die Teilnehmer die Lernziele erreicht haben. Die Tests können auch als Basis für ein Zertifikat dienen. Die für die Tests bzw. Prüfung benötigte Zeit ist nicht in den geplanten 40 Trainingseinheiten enthalten.